A full approach for Intrusion Detection in Wireless Sensor Networks

Andreas A. Strikos

School of Information and Communication Technology
KTH
Stockholm, Sweden 16453
strikos@kth.se

March 1, 2007

Abstract

Wireless Sensor Networks (WSN) are one of the hottest areas over the past few years. The number of the potential applications, involving WSNs dictates that they should be secure. In this paper we will show the major threats that WSNs have to deal with. Additionally we will mention existing countermeasures, but we will focus on intrusion detection. We combine existing IDS approaches and show the steps to build an IDS for WSNs.

1 Introduction

Wireless sensor networks (WSN) have become increasingly one of the most promising and interesting areas over the past few years. These networks may be very large systems comprised of small sized, low-power, low-cost sensor devices that collect detailed information about the physical environment. Each device has one or more sensors, embedded processor(s), and low-power radio(s), and is normally battery operated. Examining each such single device individually, might appear to have small utility. The value of sensor networks however, lies in using and co-coordinating a vast number of such devices and allows the implementation of very large sensing tasks. In a usual scenario, these networks are deployed in areas of interest (such as inaccessible terrains or disaster sites) for fine grained monitoring in various classes of applications [1]. The flexibility and self-organization, fault tolerance, high sensing fidelity, low-cost, and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the near future, this wide range of application areas will make sensor networks an integral part of life [2].

Although the research in subjects related with WSN is very productive, security in WSN still needs work. The deployment methods of WSN makes them more vulnerable to various attacks. WSN are used in applications where the sensors have physical interactions with the environment and are accessible by anyone makes them more vulnerable to security threats. The limitations [3] of WSN in memory, energy and accessibility after deploying makes the use of existing security techniques infeasible. In this paper we will mention the security threats, but we will mainly focus on using intrusion detection systems (IDS) for WSN. There are proposals for IDS in WSN, but many of them are not complete, as they only focus on a part of the IDS. Our contribution in this paper is the combination of several techniques and the creation of a new IDS, based on these technics.

The rest of the paper is organized as follows. Section 2 shows the security threats that WSN must deal with today. In section 3 we describe the existing countermeasures for these threats and in section 4 we introduce and describe the architectures of an IDS for networks. Section 5 describes an existing IDS for WSN and in section 6 we describe our complete approach for creating a WSN IDS. Finally in section 7 we conclude and discuss future work.

2 Security Threats

WSN pose unique challenges and because of this traditional security threats that all the other wireless network face can not assumed for WSN. There are many paper as [4], [5], [6], [7], [8], [9] that present the significant security problems. Here we will try to summarize all the existing threats and point out the major attacks against a WSN.

2.1 Routing Threats

The simplicity of many routing protocols for WSN make them a easy target for attacks. Karlof and

Wagner in [10] classify the routing attacks into the following categories:

1. **Spoofed, altered, or replayed routing information**
   While sending the data, the information in transit may be altered, spoofed, replayed, or destroyed. Since sensor nodes usually have only short range transmission, an attacker with high processing power and larger communication range could attack several sensors simultaneously and modify the transmitted information.

2. **Selective forwarding**
   In this kind of attack a malicious node may refuse to forward every messages it gets, acting as black hole or it can forward some messages to the wrong receiver and simply drop others.

3. **Sinkhole attacks**
   In the Sinkhole attack, the goal of the attacker is to attract all the traffic. Especially, in the case of a flooding based protocol the malicious node may listen to requests for routes, and then reply to the requesting node with messages containing a bogus route with the shortest path to the requested destination.

4. **Sybil attacks**
   In Sybil attack the compromised node presents itself as it as multiple nodes. This type of attack tries to degrade the usage and the efficiency of the distributed algorithms that are used. Sybil attack can be performed against distributed storage, routing, data aggregation, voting, fair resource allocation, and misbehavior detection[11].

5. **Wormholes**
   Wormhole attack [12] is an attack in which the malicious node tunnels messages from one part of the network over a link, that doesn't exist normally, to another part of the network. The simplest form of the wormhole attack is to convince two nodes that they are neighbors. This attack would likely be used in combination with selective forwarding or eavesdropping.

6. *HELLO* **flood attacks**
   This attack is based on the use by many protocols of broadcast *Hello* messages to announce themselves in the network. So an attacker with greater range of transmission may send many *Hello* messages to a large number of nodes in a big area of the network. These nodes are then convinced that the attacker is their neighbor. Consequently the network is left in a state of confusion.

7. **Acknowledgement**
   Some wireless sensor network routing algorithms require link layer acknowledgements. A compromised node may exploit this by spoofing these acknowledgements, thus convincing the sender that a weak link is strong or an dead sensor is alive.

2.2 Denial of Service (DoS)

This class of attacks is not concerned with the information that is transmitted. Rather, the goal of the attacker is to exhaust the resources of the networks and cause it not to function properly. Wood and Stankovic [13], [14] classify several forms of DoS attacks based on the layer that the attack uses. Some of them were already mentioned so we will not repeat them. At the physical layer the attacks take the form of jamming and tampering. Jamming has to do with interfering with the radio frequencies nodes are using. Tampering refers to the the physical altering or even damaging of the nodes. An attacker can damage and replace a node, for example, by stealing or replacing information or cryptographic keys. At the link layer the attacker can generate collisions and exhaustion may be caused from protocols that attempt retransmission repeatedly, even when triggered by an unusual and suspicious collision. Additionally unfairness threats may occur when the attacker seeks to abuse a cooperative MAC-layer priority scheme. This threat may not result a total DoS, but it could downgrade the service which others experience.

3 Countermeasures

In this section we briefly examine the existing countermeasures for the above threats. Karlof and Wagner in [10] give an analysis of the security threats in routing in WSN and propose methods to deal with each of them. Wood and Stankovic [13] studied DoS attacks and possible defenses. JAM [15] is a service for sensor networks, which detects jammed areas in the sensor networks and helps to bypass the jammed area, enabling routing within the sensor network to continue. Cagalj, et al. [16] present wormholes in WSN as a reactive defense mechanism for preventing jamming DoS attacks. SPINS [17] is a suite of security protocols optimized for sensor networks. SPINS has two secure building blocks: SNEP and TESLA. SNEP provides data confidentiality, two-party data authentication, and evidence of data freshness. TESLA on the other hand deals with authenticated broadcast for severely resource-constrained environments. TinySec

[18] is link layer security architecture for wireless sensor networks. Newsome, et al. [11] analyze the Sybil attack in WSN and propose several mechanisms for defending. Karakehayov [19] describes REWARD, a novel routing algorithm for wireless sensor networks. The algorithm is adjustable and can wage counter attacks against either single black holes or teams of malicious nodes. In [20], [21], [22] key-management and key pre-distribution schemes are introduced. Du, et al. [23] propose LEAP+ (Localized Encryption and Authentication Protocol), a key management protocol for sensor networks that is designed to support in-network processing, while at the same time restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node.

4 Intrusion Detection Systems (IDS)

Nevertheless, none of the above solutions offer protection from both inside and outside intruders. Intrusion detection systems, on the other hand, can do this. We believe that intrusion detection systems are necessary because simple security mechanisms, such as cryptography, cannot offer the needed security. For example cryptographic mechanisms provide protection against some types of attacks from external nodes, but it will not protect against malicious inside nodes, which already have the required cryptographic keys. Therefore, intrusion detection mechanisms are necessary to detect these Byzantine nodes. In this section we describe IDS architectures for widely known networks.

4.1 IDS Architectures

IDS architectures are classified into two basic categories: host-based and network-based, depending on the data collection mechanism. Host-based IDS consult several type of log files (kernel, system, application, etc.) and compare the logs against an internal database of common signatures for known attacks. Network-based IDS operate differently from host-based IDS. The design philosophy of a network-based IDS is to scan network packets, auditing packet information, and logging any suspicious packets.

Additionally, IDS architectures can further be classified based on the detection technique. Signature-based IDS centers on finding an occurrence of predefined signatures or behavior that matches a previously known malicious action or indicates an intrusion. Anomaly-based IDS check for any behaviors that fall outside the predefined or accepted model of behavior. In [24], Brutch and Ko introduce another type of IDS. Their specification-based IDS defines a set of constrains that are indicative of a program's or protocol's correct operation.

4.2 Wireless Network's IDS Architectures

Furthermore, in [24] Brutch and Ko divide wireless ad-hoc network IDS architectures into three categories. This classification can be adjusted to the needs of WSN IDS.

1. **Stand-alone**
   In this category each node operates as a independent IDS and is responsible for detecting attacks only for itself. Such an IDS does not share any information or cooperate with other systems. This architecture implies that all the nodes of the network are capable of running an IDS.

2. **Distributed and Cooperative**
   Here, all nodes still are running their own IDS, but the IDS cooperate in order to create a global intrusion detection mechanism.

3. **Hierarchical**
   In this case the network is divided into clusters with cluster-head nodes. These nodes are responsible for routing within the cluster and accept all the accusation messages from the other cluster-members indicating something malicious. Additionally, the cluster-head nodes may also detect attacks against the other cluster-head nodes of the network, as they constitute the backbone of the routing infrastructure.

5 Existing IDS models for WSN

In this section we will describe some of the existing IDS models for WSNs. The different models use several methods and architectures to build the IDS. Below we describe the basic philosophy for each of these IDS in order to understand their logic.

5.1 Self-Organized Criticality & Stochastic Learning Based IDS

Doumit and Agrawal [25] propose an anomaly approach based on the structure of naturally occurring events. This approach takes advantage of the self-organized criticality of a certain location based on a environment variable (say temperature) and uses it to detect future anomalies, by comparing new data with older data. This model uses a Hidden Markov Model, which has previously been used in network-based IDS for wired systems [26], [27]. In a Hidden Markov Model the probability of being in a certain state depends only on the previous state. Hence they are memoryless.

5.2 IDS for Clustering-based Sensor Networks

Su, et al. [28] propose two approaches to improve the security of cluster-based sensor networks using intrusion detection systems. The first approach use a model based on authentication, which can only resist outside attackers. Its basic technique is to append a message authentication code (MAC) to every message. Each time a node wants to send a message it appends to it a time stamp and a MAC is generated by the pairwise key or individual key depending on the role of the sender (cluster-head, member-node, or base station). In order for the receiver to verify the sender, the LEAP[29] security mechanism is used. As we mention above this approach only helps resistance outside attacks. The second scheme is called Energy-Saving and it also offers protection against outside attackers. This approach focuses on detecting misbehavior both in member-nodes (MN) and in cluster-head nodes (CH). Member-nodes are monitored by cluster-head node since every MN sends its data to its CH. When a misbehavior is detected the CH broadcasts an alarm message encrypted with the cluster key to restrain this specific node. CH monitoring is done with the following algorithm. First the CH decides which nodes are energy capable of monitoring the CH. This is achieved by sending messages querying the energy state of every MN. CH ignores the nodes with low energy and divides the remaining MNs into groups. Every group then monitors the CH in turn. At any moment only one group (the active group) is monitoring the CH. When a misbehavior is detected at least by X monitor nodes, then the CH is revoked.

5.3 A non-cooperative Game Approach

Agah, et al. [30] propose a game theoretic framework for defending nodes in a sensor network. The authors use three different schemes for defense. In each approach they divide the sensor network into clusters, each of which has a node as its cluster head. For every scheme they use another technique for finding which is the best cluster-head to protect using the IDS, since due to limitations in such networks we can not protect all of them. In the first scheme they define one non-operative game between the attacker and the nodes. Using game theory and more specific Nash equilibrium they decide which cluster-head to protect and so they end up with a defense strategy for the IDS. In the second scheme the Markov Decision Process(MDP) is used in order to determine the cluster-head that the IDS will protect. Knowing the past behavior of the attacker and the past states of the system we can predict using MDP which is the most vulnerable cluster-head and the most probable target of the attacker. In the third scheme things are simpler. At each time slot the cluster-head that is protected is the one with the highest traffic.

5.4 Decentralized IDS

A.P. Silva et al. [31] propose an IDS that fits the demands and restrictions of WSNs. They mention that in order to build a appropriate IDS for WSN the following steps should be followed: 1) pre-select, from an available set of rules; 2) compare the existing information from the network with the information required from the pre-select rules in order to define the final rules; 3) set the parameters of the final rules with the values of the design definitions. Additionally they provide a set of proposed rules. They also propose an algorithm that the IDS should follow. Phase one gathers the data from the incoming messages. This data will be analyzed with the help of the rules in phase two. If the analysis fails a failure is raised. If, in phase three, the number of the failures is greater than the number of the expected occasional failures in the network, then a intrusion detection alarm is raised.

6 Our Model

None of the above approaches provides a complete way to build an IDS. For example, some approaches describing their IDS using cluster techniques, but they don't mention how the cluster will be created and how it will behave. That is why we choose to combine several of the above approaches in order offer a complete IDS for a WSN.

The low energy constrains in WSN dictates the use of a hierarchical model for IDS. As we mentioned earlier this means that we will divide our network in clusters, each of which will have a cluster-head. This minimizes the energy consumption by avoiding all the nodes needing to send data to a distant base station. Consequently we utilize centralized routing, which means that every packet of transmitted data will forwarded always to cluster-head and then to the base station.

In order to form the clusters we will use the protocol described in [32]. This protocol is a "cluster-first" protocol, which means that first the clusters are formed, then the cluster-heads are elected. This protocol offers the security we need when we are creating the cluster because while external attackers can be prevented from participating in the cluster formation process, inside attackers that do not follow the protocol semantics can be identified and removed from the network. The protocol follows four basic steps and one more additional if an anomaly appears. The first step consists of the exchange of the neighbor

lists between the neighbors and the computation of the local maximum clique (cluster) by each of the nodes. In the second step, each node exchanges its local maximum clique with its neighbors, and adjust its maximum clique according to its neighbor nodes local maximum cliques. In the third step, each node exchanges the updated clique with its neighbors, and derives its final clique. In step four, the neighbors exchange their final cliques and, if a clique inconsistency is detected, it moves to fifth step. Otherwise, it terminates successfully. In the last step, each node performs conformity checking. If it identifies malicious (neighbor) nodes, it removes them from the network, and restarts the protocol from step one. Otherwise, it enforces the clique agreement and terminates. The last step has two stages. In Stage I, node i performs conformity checking to identify malicious nodes that send inconsistent messages in the previous four steps. Suppose a normal node i detects a clique inconsistency with node j. Node i requests node j to forward the messages that node j received in the first four steps. Node i, then, re-computes the first three steps of the cluster formation protocol for node j. If the derived final clique is not the same as what node i received from node j in Step 4, node j is a malicious node. If node j passes checking 1, this means that another common neighbor of nodes i and j sends different messages to nodes i and j in any step. So node i can detect the malicious node k.
When no malicious node is identified in stage I, node i enters stage II. Stage two detects silence attacks in steps two and three. When a malicious node launches silence attacks, a normal node may detect the malicious node if certain messages are not received from the malicious node. In silence attacks in step two the solution is to split nodes, that detect inconsistency, into different cliques. In silent attacks in step three, node i just removes the malicious node from its clique, since it knows that the malicious code sends its updated clique to node j, but does not send it to node i.

The next problem, that we are must deal with is the placement of the IDS. We must decide which nodes will run the IDS. The solution to our problem is described in [33]. The authors consider the set of all cluster-head and determine a set of nodes called the cut-set. Where a cut-set is a set of sensor nodes such that all paths from $c_1, \ldots, c_j$ to d traverse this set of node. Here $c_1, \ldots, c_j$ is the cluster-head nodes. So the IDS modules should be placed on all nodes that belong to the cut-set. Having a minimal number of cluster-heads makes the algorithm faster and the cut-set smaller, thus more energy efficient. If a node is judged to be abnormal by cluster-head it is restrained. This can be done by the cluster-head broadcasting an alarm message to the cluster.

Next we have to be sure that the cluster-nodes are secure and they are not malicious. Su, et al. [28] propose a way to do this monitoring. As we explained in a previous section this is done by the cluster-head deciding which nodes are energy capable to monitor it. We believe that this approach of using a rotating group of monitors will aggravate the energy consumption, so we modify this algorithm. After the cluster-head has been elected it divides the cluster into teams arbitrarily, without having to send messages that will cost energy. Then each team will monitor the cluster-head in a round-robin schedule. If the number of the nodes that indicate that cluster-head is malicious is above a threshold, then the cluster-head is revoked by the monitoring team and another cluster-head is elected.

Since our model is network based, it will detect intrusion based on the messages that it monitors. These messages can be analyzed using rules. Da Silva, et al. [31] define the necessary rules that meet the demands and restriction of WSNs. Below we present the applicable rules:

1. **Interval rule**
   a failure is raised if the delay between the arrival of two consecutive messages is larger or smaller than allowed limits
2. **Retransmission rule**
   a failure is raised when a message is not forwarded as it should.
3. **Integrity rule**
   the message payload must be the same along the path from sender to receiver
4. **Delay rule**
   the retransmission of a message must occur within a specified time
5. **Repetition rule**
   the same message can be transmitted by the same neighbor only a limited number of times
6. **Radio transmission range**
   all messages must be originated only by one of the neighbors
7. **Jamming rule**
   the number of the collisions associated with a message must be lower than the expected number in the network.

Based on these rules our IDS model will detect an intrusion. If we have a violation of these rules an alarm will be raised. If the alarms for a specific node is above a threshold, then this node is treated as an intruder and is restrained by the cluster-head. Similarly if the alarms raised by the monitoring team of the cluster-head are above threshold, then the cluster-head is revoked and restrained and a new cluster-head is elected from the beginning.

6.1 Further Comments

The centralized routing method we used has the disadvantage of not using always the best energy path to the base station. However, we assume that the cost of running IDS in every node it would be bigger than the cost of not using always the best path.

Additionally, instead of using the cluster form algorithm as in [32] we could use the algorithm of dominating sets described in [33]. This would better handle the problem with the best path because the number of hops between any node and its cluster-head should be minimal. So it would be more energy efficient. The reason that we selected our approach is because the dominating set algorithm cannot survive attacks from malicious participants in hostile environments. Malicious nodes may lie about their metrics (e.g., increase transmission power for cluster-head advertisement messages) to make themselves elected as cluster-heads. As a result, they can control all the nodes in their clusters. In contrast, the algorithm in [32] is secure and is able to handle inside attackers. Thus we choose this because security seems to be one the most significant problems in WSNs. Whereas, technology and energy capacity in WSNs seems to improve in contrast with the security.

One of the most significant issues about a WSN, that we have to always keep in mind is that in the real world may not work as we are expecting. Chatzigiannakis, et al. [34] show us that the results of the simulations may differ a lot from that of real experiments. Although the approaches that we choose to combine have been separately tested with simulators and the results are satisfactory, the experiment results may be different. Also, without experimental evaluation we can not know the cost of our proposed IDS for WSN as a security solution.

7 Conclusions & Future Work

The goal was to present the significance of the security nowadays in WSN. We indicated security threats that WSN are vulnerable to and we mention some existing countermeasures. We focused on IDS and propose our own model that combines already existing approaches, in order to provide a more complete solution. In the future, we should test our model with simulation or even better with real experiments. It would be very interesting to know what is the real cost of IDS in WSN.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks : a survey", *Computer Networks, 38:393-422, 2002.*

[2] J. Kahn, R. Katz, and K. Pister, "Next century challenges : Mobile networking for smart dust", *In 5th ACM/IEEE Annual International Conference on Mobile Computing (MOBICOM 1999), pages 271278, 1999.*

[3] U. Bilstrup, K. Sjöberg, B. Svensson, and P-A. Wiberg, "Capacity Limitations in Wireless Sensor Networks", *Proc.of ETFA2003, 9th IEEE International Conference on Emerging Technologies and Factory Automation, Lisbon, Portugal, 16-19 September 2003*

[4] R. Roman, J. Zhou, and J. Lopez, "On the Security of Wireless Sensor Networks", *Proceedings of 2005 ICCSA Workshop on Internet Communications Security, pp 681-690, LNCS 3482, Singapur, May 2005.*

[5] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", *In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (Anchorage, AK, May 11, 2003).*

[6] A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks", *Computer, v.35 n.10, p.54-62, October 2002*

[7] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", *Proceedings of the 9th ACM conference on Computer and communications security, November 18-22, 2002, Washington, DC, USA*

[8] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks", *Communications of the ACM, Volume 47 , Issue 6 (June 2004)*

[9] A.S.K. Pathan, H-W. Lee, and C. S. Hong, "Security in wireless sensor networks: issues and challenges", *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, Vol.2, Iss., 20-22 Feb. 2006*

[10] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures", *In Proc. of First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.*

[11] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses", *Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 268.*

[12] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," *Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.*

[13] A. Wood and J. Stankovic, "Denial of service in sensor networks", *IEEE Computer, pages 5462, Oct. 2002.*

[14] A. D. Wood, J. A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press, 2004 (invited paper).*

[15] A.D. Wood, J.A. Stankovic, and S.H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks", *24th IEEE Real-Time Systems Symposium, RTSS 2003, pp. 286-297.*

[16] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti-Jamming Techniques in Sensor Networks", *in IEEE Transactions on Mobile Computing, January 2007*

[17] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", *Wireless Networks, vol. 8, no. 5, 2002, pp. 521-534.*

[18] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks", *Proc. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, 2004, pp. 162 175.*

[19] Z. Karakehayov, "Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks", *Proceedings of the Workshop on Real-World Wireless Sensor Networks REALWSN'05, Stockholm, Sweden, June 2005*

[20] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks", *In IEEE Symposium on Security and Privacy, Berkeley, California, May 11-14 2003, pp. 197213.*

[21] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", *Proc. ACM CCS'02, 18-22 November 2002, pp. 41-47.*

[22] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks", *Proc. of the 10th ACM conference on Computer and communications security, 2003, pp. 42-51.*

[23] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks", *ACM Transactions on Sensor Networks (TOSN), Volume 2 , Issue 4 (November 2006), Pages: 500 - 528*

[24] P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks" *in Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on, pp. 368373, 2003.*

[25] S. Doumit and D.P. Agrawal,"Self-organized criticality & stochastic learning based intrusion detection system for wireless sensor network", *MILCOM 2003 - IEEE Military Communications Conference, vol. 22, no. 1, pp. 609-614, 2003*

[26] D. Ourstou, S. Matzner, W. Stump, B. Hopkins, and K. Richards, "Identifying Coordinated Internet Attacks", *Proceedings of the Second SSGRR Conference. Rome, Italy, 2001.*

[27] H.-J. Park and S.-B. Cho, "Privilege Flows Modeling for Effective Intrusion Detection based on HMM", *Department of Computer-Science, Yonsei University, Seoul 120-749, Korea.*

[28] C.-C. Su, K.-M. Chang, Y.-H. Kuo, and M.-F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", *in 2005 IEEE Wireless Communications and Networking Conference, WCNC 2005: Broadband Wirelss for the Masses - Ready for Take-off, Mar 13-17 2005.*

[29] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", *In The Proceedings of the 10th ACM conference on Computer and communications security, 2003.*

[30] A. Agah, S. Das, K. Basu, and M. Asadi, "Intrusion detection in sensor networks: A non-cooperative game approach", *in 3rd IEEE International Symposium on Network Computing and Applications, (NCA 2004), Boston, MA, August 2004, pp. 343346.*

[31] A. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. Wong, "Decentralized intrusion detection in wireless sensor networks", *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobilenetworks- 2005.*

[32] K. Sun, P. Peng, P. Ning, and C. Wang, "Secure Distributed Cluster Formation in Wireless Sensor Networks", *in Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC'06), Pages: 131-140, December 2006.*

[33] F. Anjum, D. Subhadrabandhu, S. Sarkar, and R. Shetty, "On Optimal Placement of Intrusion Detection Modules in Sensor Networks", *1st International Conference on Broadband Networks (BROADNETS04), October 2004.*

[34] I.Chatzigiannakis, S.Nikoletseas, and A.Strikos, "Experimental Evaluation of the Performance of Multi-hop Wireless Sensor Networks", *In Proc. 5th IEEE Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP'06), Patras, Greece, July 19-21, 2006, pp. 579-582.*